Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS Data Classification and Handling Policy

Version Control

Document title: GBS Data Classification and Handling Policy	**No of pages:** 9
Version Number: V1.0	**Date first published:** April 2021
Approved by: Resource Committee	**Last review date:** January 2022
Date originally approved: February 2022	**Due for next review: January 2023**

Related policies
▪ GBS Records Management and Retention Policy ▪ GBS Data Protection Policy ▪ GBS Privacy Policy ▪ GBS Data Subject Access Request Policy ▪ GBS Equality and Diversity Policy ▪ GBS Access Control Policy ▪ GBS IT Security Policy ▪ GBS Email Usage Policy
External Reference
1. Information Commissioner's Office, Accessed online at: https://ico.org.uk/ 2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted 3. UK Public General Acts, *Equality Act 2010*, Accessed online at: https://www.legislation.gov.uk/ukpga/2010/15/contents

GLOBAL APPLIED KNOWLEDGE

Contents

Global Banking School Data Classification and Handling Policy

1. Purpose and Scope

1.1 Global Banking School (GBS) needs to collect, store and process personal data about its staff, students, and other individuals it has dealings with, to carry out our functions and activities. GBS is a controller for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation including The Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK GDPR).

1.2 This policy outlines the types of data and provides instruction on the classification to be applied and how it may be handled. Without appropriate classification and labelling, data will likely be inconsistently managed. This inconsistency may lead to sensitive data being processed in inappropriate ways, potentially leading to a damaging data breach. A breach may result in unlimited fines and severe reputational damage to GBS.

2. Roles and Responsibilities

2.1 Global Banking School is registered with the Information Commissioner's Officer as a Data Controller. Details of the School's registration are published on the Information Commissioners website. GBS as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK GDPR and DPA (2018). Roles and responsibilities include:

- GBS Senior Management Team (SMT): Responsible for ensuring that their staff are made aware of this policy and that breaches are dealt with appropriately and developing and encouraging good information handling practices within their areas of responsibility.

- Data Owners are responsible for classification. GBS SMT and faculties are commonly considered data owners. It is their responsibility to discover and label information according to its sensitivity. However, data owners can be more broadly defined as those that create the data e.g., researchers collecting data in the field. Regardless all data owners must classify and

appropriately label data according to GBS Data Classification and Handling Policy.

- Information Commissioner's Office ("ICO"): ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

- Data Protection Officer**:** DPO is responsible for advising GBS on its obligations, monitoring compliance, assisting with Data Protection Impact Assessments (DPIAs) and liaising with the Information Commissioner's Office. The DPO is also responsible for ensuring that GBS processes the personal information of its staff, students, customers, providers, and partners in compliance with the applicable data protection rules. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

- GBS Academic Standards and Quality Office (ASQO)[1]**:** Responsible for implementation, monitoring and review of this policy and ensuring that training, guidance, and advice regarding data protection compliance is made available to staff and can be contacted on asqo@globalbanking.ac.uk.

- IT Department**:** IT are responsible for ensuring that advice and guidance on technical specifications and technical security measures are made available to staff such as the use of IT Security Policy.

- Line Managers: Responsible for ensuring that their staff have completed all required training in Data Protection. Ensuring that activities requiring a Data Protection Impact Assessments (DPIA) are referred to the DPO. Ensuring that requests made under data subject rights are referred to Human

[1] *Formerly known as GBS Quality Assurance Team*

Resources/DPO ensuring that suspected or actual compromises of personal data are reported immediately.

- GBS Staff: Responsible for complying with Data Protection Policy. Completing all required data protection training including refresher training as and when required. They must ensure that they are processing data in line with GBS policies and requirements.

- All GBS Members (staff and students)-Responsible for ensuring that *any* personal data that they supply about themselves to GBS are accurate and up to date. All members of staff and students are advised to familiarise themselves with the appropriate GBS Data Protection Policy. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

3. Defining a Classification

3.1 Classification is the process of analysing and labelling data (digital, paper or otherwise) according to the impact a compromise of its confidentiality, integrity and/or availability would have on GBS. The greater the impact, the higher the classification.

3.2 Data classification enables efficient processing of data. If data is not classified, it would be necessary to handle all data as if it was highly sensitive to comply with legal requirements. This results in restrictive protections, creating unnecessary demands to many common tasks. Unnecessary restrictions can slow and frustrate completing primary operational tasks. By appropriately labelling data in combination with controls selected to balance both data protection obligations and the need to reduce friction, greater compliance and security will be achieved.

4. Data Classifications

4.1 GBS has five information classifications to help staff identify the level of security the information requires. The five classifications include: Public, Restricted, Private, Internal and Confidential.

4.2 **Public**

4.2.1 Information that is produced for publication and/or could be disclosed with no impact on GBS can be labelled as Public. It is important to note that although the confidentiality of this category does not need to be maintained the integrity and appropriate availability must be. For instance, a press release on an emerging infectious disease is designed to reach a wide audience and so the confidentiality does not need maintaining. However, the integrity of the message is vital to maintain to prevent reputational damage. Availability in this instance is very important too. As if the data is not available, the objective will fail.

4.3 **Restricted**

4.3.1 This highest level of classification is reserved for the most sensitive of data. Access to this data must be limited to specific named individuals having to work in an appropriately restricted manner. Compromised of this data may result in significant legal liability, severe distress/danger to individual(s), severe damage to organisational reputation and/or significant loss of asset value. Personal health data such as medical records about identifiable individuals are a common example of this highly sensitive category.

4.4 **Private**

4.4.1 Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms and must be protected if it contains sensitive information. For example, emails to colleagues regarding work buffets or quizzes or personal information relating to that individual.

4.5 **Internal**

4.5.1 Internal classified data can be characterised as non-sensitive, organisational data. If this level of data has any of its security properties violated it will have a low impact. Access is limited to GBS members and other authorised users. Disclosure may result in temporary inconvenience to individual(s) or organisation(s) or minor damage to reputation that can be recovered and has a small containment cost. Some common examples are project documentation, anonymised data that cannot be re-identified,

organisational information that is appropriate for GBS staff and students only, staff training materials and non-sensitive committee minutes etc.

4.6 **Confidential**

4.6.1 Confidential data is the most common sensitive data processed. Access must be limited to specific named individuals. Disclosure may cause significant upset to individuals, reputational damage and/or financial penalty. Common examples may include interview notes, disciplinary correspondence, staff salaries, exam board minutes, datasets with sensitive personal data, student demographic details and assessments, staff appraisals and assessments, internal and external audit reports etc.

5. Related Policies

5.1 This policy is accompanied by the Staff Handbook and must be followed to achieve GBS policy objectives. Reference should also be made to the, GBS Data Protection Policy, GBS Privacy Policy, GBS Data Subject Access Request Policy, GBS Records Management and Retention Policy, GBS IT Security Policy, and GBS Equality and Diversity Policy. Information on other related policies is available from GBS Academic Standards and Quality Office (ASQO) and can be found under the GBS General Policies folder on SharePoint.

6. Audit and Compliance

6.1 GBS Data Classification and Handling Policy may be amended by GBS at any time.

7. Alternative Format

7.1 This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk

Annex 1 – GBS Information Classifications

GBS has five information classifications to help staff identify the level of security the information requires. The five classifications include: Public, Restricted, Private, Internal and Confidential.

CLASSIFICATION	DEFINITION
Public	Data that can be freely disclosed to the public. Examples include GBS contact information, location, job descriptions and prospectus.
Restricted	Highly sensitive internal data. Disclosure could negatively affect operations and put GBS at financial or legal risk. Restricted data requires the highest level of security protection by everyone working at GBS from staff to students to partners etc. For example, Committee papers and documents marked for the attention of a specific reader.
Private	Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms. For example, emails to colleagues regarding work buffets or quizzes etc.
Internal	Data that has low security requirements, however, is not meant for public disclosure such as marketing research, academic handbooks.
Confidential	Confidential information is information shared with only a few people, for a designated purpose and can be shared with others within GBS. The person who is receiving the information from you, the receiver, generally cannot take advantage and use your information for their personal gain, such as giving the information out to unauthorised third parties. These can include documents prepared for publication or unpublished research data.